Department of Homeland Security Daily Open Source Infrastructure Report for 09 June 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- ComputerWorld reports the American Institute of Certified Public Accountants has confirmed that a computer hard drive containing the unencrypted names, addresses, and Social Security numbers of nearly all of its 330,000 members has been missing since February. (See item 7)
- The Associated Press reports a Saudi man faces charges he threatened to blow up a Delta Air Lines flight because he was upset he was denied a job as an interpreter for U.S. military operations in Iraq. (See item 15)
- USA TODAY reports a Police Foundation report has concluded major shopping centers have ranked near the top of potential terrorist targets, but there has been scant investment in additional security and emergency response plans are woefully inadequate. (See item 38)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *June 08, Associated Press* — **Energy issues to top G−8 talks in Russia.** Oil prices and energy policy are likely to stay at the center of debate this week as finance ministers from the world's major industrial nations meet in St. Petersburg, Russia, to consider how soaring energy prices are affecting the global economy. Russian Finance Minister Alexei Kudrin said ministers

meeting Friday, June 9, and Saturday, June 10, would review the effect of the higher costs on poorer nations, as well as the role played by the World Bank and International Monetary Fund in easing their woes. The G−8 countries −− the U.S., Japan, Germany, France, Britain, Italy, Canada and Russia −− have called for better data on oil production and reserves to help markets function more efficiently. They also have urged G−8 oil producers to use their surging profits to boost global production.
Source: http://www.chron.com/disp/story.mpl/ap/fn/3949154.html

2. *June 07, Washington Post* — **U.S. science panel sees big problems if Indian Point reactors are closed.** Closing the Indian Point nuclear reactors would make electricity more expensive, leave New York more vulnerable to natural gas shortages, and add to pollution, according to a report released on Tuesday, June 7 by a committee of the National Academy of Sciences. The committee said that there were no insurmountable technical obstacles to closing the plant. But it asserted that electric demand was growing so fast in the region, and building power plants was so difficult, that simply meeting power needs during peak periods would be a challenge even if the reactors stayed in operation. Congress provided funding for the study, under a bill sponsored by Nita M. Lowey, a Westchester, NY, Democrat who says the reactors should be closed because of the risk of a release of radiation through accident or terrorist attack. At the moment building any power plant in New York State is difficult, the report said, because a law that laid out the process for environmental reviews and permits for new plants was allowed to expire in 2003. The amount of generating capacity under construction now is inadequate to meet peak demand in 2009, and the shortfall will be far larger if Indian Point closes, the report said.
National Academy of Sciences Report: http://www.nap.edu/catalog/11666.html
Source: http://www.nytimes.com/2006/06/07/nyregion/07indian.html?_r= 1&oref=slogin

[Return to top]

Chemical Industry and Hazardous Materials Sector

3. *June 08, Associated Press* — **Ruptured gas line prompts evacuations in Maryland.** A ruptured gas line in Montgomery County, MD, Thursday, June 8, prompted an evacuation of 45 homes in a Germantown neighborhood. The cause of the leak is under investigation and it's unclear how long it will take to repair the damage.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/06/08/AR2006060800701.html

[Return to top]

Defense Industrial Base Sector

4. *June 07, Defense News* — **Air Force cuts weather satellite capabilities to keep program moving.** When the U.S. government restructured its proposed weather satellite network, capability took a back seat to continuity. The Pentagon decided Monday, June 5, to go forward with the National Polar−orbiting Operational Environmental Satellite System (NPOESS), choosing options that would make the system cost about $11.5 billion, about $2.5 billion less

than had been estimated in January, said Gary Payton, Air Force deputy undersecretary for space programs. The first NPOESS satellite won't carry the Conical Microwave Imager/Sounder, a large microwave sensor that was intended to see through clouds to measure wind speeds and directions by their effects on water. The rotating sensor threatened to interfere with the nearby visible/infrared imager/radiometer suite sensor. The Air Force will ask for new bids on the satellite later, Payton said.
Source: http://www.defensenews.com/story.php?F=1855395&C=america

5. *June 07, Government Computer News* — **DoD moves forward with portal.** The Army and the Defense Information Systems Agency (DISA) are moving forward with the vision of a single enterprise service online portal for all of the Department of Defense (DoD). Along with representatives from the Navy, Air Force and the other military agencies, the Army and DISA are leading the working groups to create the initial requirements and standards, and figure out what existing components can be reused to develop the Defense Knowledge Online (DKO) portal. John Garing, DISA CIO, said there are some challenges to making DKO happen, including ensuring that it can scale to the number of users and that the contracting language is appropriate.
Source: http://www.gcn.com/online/vol1_no1/40968-1.html

[Return to top]

Banking and Finance Sector

6. *June 08, Register (UK)* — **ID scammers pose as online businesses.** Access Business Communications (abc), a Scottish business telecom retailer, was recently targeted by identity scammers on Alibaba.com, a reputable Website that brings together suppliers and buyers of products made in China. The scam came to light after abc discovered bogus profiles in the name of "Access Business Communications Ltd" and "Freedom Mobiles," on Alibaba.com. The rogue profiles touted offers for high value products such as mobile phones, laptops and plasma screen televisions. The conmen posing as abc sought to convince users to send money by Western Union transfer for goods they will never receive.
Source: http://www.theregister.co.uk/2006/06/08/corporate_id_fraud/

7. *June 07, ComputerWorld* — **AICPA group says hard drive with data on 330,000 members missing.** Adding to the lengthening list of organizations reporting data compromises, the American Institute of Certified Public Accountants (AICPA) Wednesday, June 7, confirmed that a computer hard drive containing the unencrypted names, addresses and Social Security numbers of nearly all of its 330,000 members has been missing since February. The hard drive had been accidentally damaged by an AICPA employee and was sent out for repair to an external data-recovery service in violation of the AICPA's policies, said Joel Allegretti, a spokesperson for the New York-based organization. It was on its way back to the AICPA via FedEx but failed to arrive. It took the organization until March 31 to "recreate the drive" and determine what data it contained. The AICPA began notifying affected members of the potential compromise of their personal data on May 8 and has since completed the task.
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9001030

8. *June 07, Websense Security Labs* — **Phishing Alert: Hapo Community Credit Union.** Websense Security Labs has received reports of a new phishing attack that targets customers of Hapo Community Credit Union. Users receive a spoofed e−mail message, which claims that they must update their account services details or the account will be suspended. This message provides a link to a phishing Website that prompts users to enter account information.
Source: http://www.websense.com/securitylabs/alerts/alert.php?AlertI D=506

9. *June 07, Websense Security Labs* — **Phishing Alert: Fox Chase Bank.** Websense Security Labs has received reports of a new phishing attack that targets customers of Fox Chase Bank. Users receive a spoofed e−mail, which claims that recent security improvements to the bank's servers require users to verify their account information.
Source: http://www.websense.com/securitylabs/alerts/alert.php?AlertI D=507

10. *June 07, Websense Security Labs* — **Phishing Alert: Industrial and Commercial Bank of China.** Websense Security Labs has received reports of a new phishing attack that targets customers of Industrial and Commercial Bank of China, ICBC (Asia). Users are lured to the fake Website, and are asked to provide login details such as user−ID and password.
Source: http://www.websense.com/securitylabs/alerts/alert.php?AlertI D=508

11. *June 07, Virgin Islands Daily News* — **Error puts students' personal data online.** A document containing Social Security numbers and other personal information belonging to nearly 250 University of the Virgin Islands (UVI) students is mistakenly accessible through an Internet search engine. Tina Koopmans, UVI vice president for information and technology services, said the document, which appears to be a student roster, was saved to the university's server by a UVI faculty member and became viewable on the Internet. "It was basically user error," Koopmans said. It is not clear how long the document has been available on the Internet, Koopmans said.
Source: http://www.virginislandsdailynews.com/index.pl/article_home? id=17591734

12. *June 05, SC Magazine (UK)* — **New IM worm targets MySpace users.** Security teams have discovered a new instant messenger (IM)−based phishing attack aimed at users of the popular social networking site MySpace. The scam begins when AOL IM users receive a hyperlink promising new photos from someone in their contact list. But clicking the link leads the victim to a bogus California−based Website that spoofs the MySpace.com log−in page, according to a Websense Security Labs alert. The fraudulent site captures MySpace usernames and passwords, and then forwards users to the real site.
Websense Security Labs alert: http://www.websense.com/securitylabs/alerts/alert.php?AlertI D=504
Source: http://www.scmagazine.com/uk/news/article/562729/new+im+worm +targets+myspace+users/

13. *June 01, Websense Security Labs* — **Phishing Alert: UCF Federal Credit Union.** Websense Security Labs has received reports of a new phishing attack that targets customers of UCF Federal Credit Union. Users receive a spoofed e−mail, which claims that their Visa card needs to be secured or will otherwise be deactivated. The message provides a link to a phishing Website that requests customers' card information.
Source: http://www.websense.com/securitylabs/alerts/alert.php?AlertI D=505

[Return to top]

Transportation and Border Security Sector

14. *June 08, Rocky Mountain News (CO)* — **Frontier to add Mexico flights.** Frontier Airlines will boost flights from Denver to Mexico by roughly 30 percent this winter holiday season as it continues to carve a niche internationally while facing more competition on domestic routes. The Denver−based carrier plans to add 13 flights a week from mid−December to early January −− one of the peak travel times to Mexico −− compared with the same period a year earlier. New service includes seven additional weekly flights to Cancún and two each to Puerto Vallarta, San Jose del Cabo and Cozumel. Frontier, Denver's second−largest carrier has found a fast−growing market in Mexico during the past few years and now offers daily nonstop service from several U.S. cities to seven resort destinations south of the border. Aside from Mexico, Frontier plans to add one daily flight from Denver to both Chicago and Dallas and switch to larger planes on some routes this fall.
Source: http://www.rockymountainnews.com/drmn/airlines/article/0,2777,DRMN_23912_4758581,00.html

15. *June 07, Associated Press* — **Saudi charged with threatening flight.** A Saudi man faces charges he threatened to blow up a Delta Air Lines flight because he was upset he was denied a job as an interpreter for U.S. military operations in Iraq. A federal magistrate ordered Saleh Suwailem, 45, of Boise, ID, held by the U.S. Marshal's Service after a hearing Tuesday, June 6, in Columbus, GA. According to a criminal complaint, Suwailem was at Georgia's Fort Benning on Monday, June 5, where he was going through the process to become an Arabic interpreter for a communications division that contracts to hire interpreters for operations in Iraq. After he was told he would not be hired because he was denied security clearance and that he would have to fly home to Idaho the next day on a Delta flight, he started drinking with some acquaintances, the complaint says. "Okay, I'm going to bomb the plane," he blurted out, according to the complaint. When he was questioned by Fort Benning officials about the remark, he said it was a joke and that he did not actually plan to bomb the flight. The FBI was alerted and Suwailem was arrested.
Source: http://www.cnn.com/2006/US/06/07/saudi.threat.ap/index.html

16. *June 07, Chicago Tribune* — **United ending Midway service.** United Airlines is pulling out of Midway International Airport, following a similar move announced last month by American Airlines. United restarted commercial service from Midway last year, but a lack of business prompted the withdrawal, Robin Urbanski, spokesperson for the carrier, said Tuesday, June 6. United's last flight from Midway will be on September 5. In May, American Airlines announced it will cease its service from the Southwest Side airport on September 1. The loss of American, followed by United's departure a few days later, is more symbolic than substantive for the local aviation market. Both airlines offer hundreds of daily flights from O'Hare International Airport, but each has only five daily departures from Midway. Neither accounts for more than one percent of the passenger market share at Midway, according to the city's Department of Aviation. Southwest Airlines dominates with 71 percent of the Midway market, followed by ATA Airlines with 11.2 percent, and AirTran Airways with 6.3 percent.
Source: http://www.chicagotribune.com/business/chi−0606070216jun07,1

,62937.story?ctrack=1&cset=true

17. *June 06, Associated Press* — **Airlines continue overseas focus.** Big U.S. airlines continue to focus their growth overseas, putting most of their new capacity in routes to Europe, Latin America, and Asia. International capacity is growing across most big airlines, while domestic capacity is either growing more slowly or shrinking, according to airlines' May traffic reports. Fliers are taking advantage: The strongest traffic growth has been for travel overseas. Airlines have long been talking about the need to reduce domestic capacity, hoping it would allow them to raise fares to cover persistently high fuel costs. Among the big airlines, United Airlines was the anomaly. It shrank its international capacity while growing in North America in May. United does not break out domestic capacity from its North America figures. Among low−cost carriers, who fly mostly domestically, Southwest Airlines Co. reported May traffic grew 13.7 percent on 7.1 percent capacity growth.
Source: http://biz.yahoo.com/ap/060606/airline_traffic_roundup.html? .v=1

[Return to top]

Postal and Shipping Sector

18. *June 07, DMNews* — **UPS enhances TradeAbility tool.** United Parcel Service (UPS) has made improvements to its TradeAbility global trade management tool, including a “screener” that automatically alerts shippers if they are trying to send a package to a person, organization, or country under official government restriction. The upgraded Denied Party Screener tool, unveiled June 6, at the Internet Retailer Conference in Chicago, helps customers comply with government trade regulations by identifying restricted trading partners before goods are shipped. Without a tool like this customers run the risk of customs seizing packages. TradeAbility’s Denied Party Screener tool relies on more than 25 U.S. government lists, and 10 non−U.S. lists, for its source information. That automates the process for shippers and eliminates the need to consult each list individually. The international sources include lists published by the United Nations, Interpol, Canada and Japan. UPS monitors these lists daily for up−to−date results. UPS TradeAbility is a Web−based management tool that helps international shippers manage the customs clearance processes.
Source: http://www.dmnews.com/cms/dm−news/direct−mail/37004.html

[Return to top]

Agriculture Sector

19. *June 08, Agricultural Research Service* — **Continuing the fight against cattle ticks.** An innovative device called a "four−poster" and chemical "tickicides" are two tools Agricultural Research Service (ARS) scientists are using to protect the southern U.S. border from ticks that carry serious cattle disease. The southern cattle tick (Boophilus microplus) and the cattle−fever tick (B. annulatus) transmit the two species of blood parasites (Babesia bovis and B. bigemina) that cause the cattle diseases known as cattle fever, Texas fever or bovine babesiosis. Before their eradication in 1943, tick−carried diseases crippled the U.S. cattle industry. Today, descendants of the ticks that caused those losses can still be found in Mexico. To keep them

out, inspectors maintain constant vigilance at the border, preventing infested cattle from entering the U.S. To combat the spread of ticks by wildlife, ARS scientists developed and patented the four−poster device that attracts mostly white−tailed deer −− the main secondary hosts for cattle fever ticks in southern Texas −− with whole−kernel corn. When a deer feeds, its head and neck brush against pesticide−saturated rollers. Later, when it grooms itself, the pesticide spreads enough to protect its entire body.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

20. *June 07, U.S. Department of Agriculture* — **Citrus canker compensation announced.** U.S. Department of Agriculture (USDA) Secretary Mike Johanns Wednesday, June 7, announced $100 million in additional funding to continue compensating commercial citrus growers in Florida for losses resulting from citrus canker eradication efforts and an interim rule that establishes the eligibility of nursery owners for these funds. With this announcement, USDA has provided a total of approximately $536 million in compensation that will go to producers and nursery owners affected by citrus canker and brings USDA closer to addressing all outstanding compensation claims.
Source: http://www.usda.gov/wps/portal/usdahome?contentidonly=true&contentid=2006/06/0196.xml

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

21. *June 08, Boston Globe* — **Massachusetts to tighten water use.** As Boston's western suburbs have grown, their demand for water has grown, too. Now, concerned that the region's supply is being stretched too thin, state officials are preparing to set new limits on water use in a number of communities along the Charles River, including Bellingham, Dover, Franklin, Holliston, Medway, Medfield, Milford, Millis, Natick, Norfolk, and Wrentham. The new standards, which are expected to hit the communities over the next several months, could mean tighter restrictions on nonessential water use. But many local officials are fighting back, arguing that the new rules will do little to replenish the regional water supply and will cost communities time and money. Many also say they were not properly consulted when the state was drawing up the rules.
Source: http://www.boston.com/news/local/articles/2006/06/08/state_to_tighten_water_use/

22. *June 08, Times−Picayune (LA)* — **Millions of gallons of water seeping away.** About 85 million gallons of drinking water −− more than two−thirds of the total pumped into the pipes −− are leaking into the ground every day through breaks in New Orleans' hurricane−fractured water system. Given the difficulty of locating underground leaks, especially with so few residents around to report them in the hardest−hit neighborhoods, Sewerage & Water Board Executive Director Marcia St. Martin said much work still must be done. Before Hurricane

Katrina, New Orleans' 455,000 residents used about 120 million gallons of water every day, St. Martin said. About 30 percent of that regularly disappeared through cracks in the ground or pooled in the street or was expended for firefighting or other public uses. Now, with the population estimated to have reached 221,000, the water board is pumping out more drinking water than before the storm only to see the bulk of it vanish underground. St. Martin said crews have repaired more than 17,000 leaks since August 29, but most of the remaining fissures are hidden beneath the streets.
Source: http://www.nola.com/news/t-p/frontpage/index.ssf?/base/news-5/1149752801307650.xml&coll=1

[Return to top]

Public Health Sector

23. *June 08, BBC News* — **Fresh bird flu outbreak in China.** A new outbreak of bird flu has been discovered in poultry in the Chinese region of Xinjiang, according to the country's agriculture ministry. The H5N1 strain was discovered in birds in Hetian County. Several cases have been reported in wild birds in recent months, but the last outbreak in poultry was reported in February, in the province of Anhui. China confirmed its first human bird flu death in November. Twelve Chinese people are now known to have died from the virus.
Source: http://news.bbc.co.uk/2/hi/asia-pacific/5057964.stm

24. *June 08, Reuters* — **Namibia plans mass polio vaccination.** The Namibian government said on Thursday, June 8, it would begin a mass vaccination campaign to combat a deadly polio outbreak after supplies of vaccine are airlifted into the southwestern African nation later this month. Seven people have died and another 27 have been infected with polio in Namibia in the past month. Namibia's ministry of health plans to begin inoculating people on June 21 using the monovalent Oral Polio Vaccine. On Wednesday, June 7, the World Health Organization said the strain involved in the Namibian outbreak had been imported from Angola.
Global Polio Eradication Initiative: http://www.polioeradication.org/
Source: http://today.reuters.com/news/newsArticle.aspx?type=healthNews&storyID=2006-06-08T140826Z_01_L08795448_RTRUKOC_0_US-NAMIBIA-POLIO.xml&archived=False

25. *June 07, Associated Press* — **States should aim to contain bird flu.** States preparing for a possible bird flu outbreak should focus on how to contain the virus because a vaccine will be unavailable for several months, the head of the U.S. Centers for Disease Control and Prevention said Wednesday, June 7. The preparation could help medical centers, which are likely to experience shortages in staffs, supplies, beds and medicine in the event of a pandemic, Julie Gerberding said. U.S. Department of Health and Human Services Secretary Mike Leavitt said that local officials would be responsible for distributing vaccine doses once they're available.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2006/06/07/AR2006060702384.html

26. *June 07, U.S. Department of Health and Human Services* — **Funding for states' bioterrorism preparedness.** U.S. Department of Health and Human Services (HHS) Secretary Mike Leavitt

Wednesday, June 7, announced that the department has made available another $1.2 billion to the states, territories, and four metropolitan areas to help strengthen their capacity to respond to terrorism and other public health emergencies. The funds will be used to improve infectious disease surveillance and investigation, enhance the preparedness of hospitals and the health care system to deal with large numbers of casualties, expand public health laboratory and communications capacities and improve connectivity between hospitals, and city, local and state health departments to enhance disease reporting. The funds will also be used to exercise existing response plans, test capabilities and evaluate improvements. HHS' Centers for Disease Control and Prevention (CDC) is providing $766 million to develop emergency−ready public health departments by upgrading, improving, and sustaining their preparedness and response capabilities for "all−hazards" public health emergencies, including terrorism and other naturally−occurring public health emergencies. HHS' Health Resources and Services Administration (HRSA) is providing $450 million for states to develop medical surge capacity and capability to deal with mass casualty events. This includes the expansion of hospital beds, development of isolation capacity, identifying additional health care personnel, and establishing hospital−based pharmaceutical caches.
Source: http://www.hhs.gov/news/press/2006pres/20060607.html

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

27. *June 08, Government Accountability Office* — **GAO−06−712: Hurricanes Katrina and Rita: Coordination Between FEMA and the Red Cross Could Be Improved for the 2006 Hurricane Season (Report).** The Red Cross played a key role in providing relief to victims of Hurricanes Katrina and Rita, mounting its largest ever disaster response. Under the National Response Plan and its emergency support function−6 (ESF−6), the Red Cross and the Federal Emergency Management Agency (FEMA) are tasked with working together to coordinate federal mass care assistance in support of voluntary organizations, as well as state and local governments, as they meet mass care needs—such as shelter, food, and first aid. Questions have been raised about how the Red Cross and FEMA operated following the Gulf Coast hurricanes and what improvements can be made for the 2006 hurricane season. This report includes the Government Accountability Office's (GAO) interim findings on the Red Cross and FEMA's hurricane operations. GAO will continue to analyze federal and charitable hurricane relief efforts. GAO recommends that 1) FEMA work with the Red Cross to reach agreement on 2006 hurricane season operating procedures, 2) the Red Cross implement staffing strategies that would improve working relationships and retention of institutional knowledge, and 3) that FEMA obtain the Red Cross's input when developing its resource tracking system. FEMA had no comments on the recommendations. The Red Cross endorsed or is taking actions, as applicable, to address the recommendations.
Highlights: http://www.gao.gov/highlights/d06712high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−712

28. *June 07, WTOC−TV (SC)* — **South Carolina emergency officials drill for hurricane evacuation.** Emergency management officials in South Carolina are making sure the state is prepared by conducting a statewide drill. The Beaufort County Emergency Operations Center (EOC) was a busy place on Wednesday, June 7, as emergency officials from around the county prepared for Isabella, a simulated category 4 hurricane headed for Charleston. When a massive evacuation was ordered, emergency officials evacuated and relocated the EOC in Beaufort to Jasper County and set up shop. Although both Beaufort and Jasper Counties did experience some trouble with their communication and technology systems, they worked through their problems just like they would have in any real emergency.
Source: http://www.wtoctv.com/Global/story.asp?S=5001762

29. *June 07, Corsican Daily Sun (TX)* — **City, county officials in Texas to participate in disaster drill.** Local emergency planners and government leaders in North Texas are going to be in a classroom from June 20 to June 22, participating in a regional exercise testing preparedness in the event of a regional emergency. The exercise will involve 12 counties and is designed to simulate a weapons of mass destruction event in the area. “Such an event could be chemical or biological in nature, and we’ll be testing our local planning procedures, communications and knowledge of our first responders,” explained Eric Ryan Meyers, who heads up the Navarro County Local Emergency Planning Committee.
Source: http://www.corsicanadailysun.com/news/local_story_158102601. html

30. *June 06, Hot Springs Star (SD)* — **Local and county disaster teams participate in mock drill in South Dakota.** One young U.S. Forestry Service (USFS) person was “killed” and two others were rendered very ill on Wednesday, June 7 as local disaster team members conducted a mock Weapons of Mass Destruction (WMD) drill at the Forestry Headquarters in Hot Springs, SD. At one point during the exercise, USFS firefighters were challenged with a “deceased” co−worker lying in a garage, soaked in an unknown liquid. When no one could identify the liquid in the garage, they requested the support of the South Dakota National Guard’s 82nd Civil Support Team (CST) from Camp Rapid in Rapid City. The job of the CST, according to Major John Emick, commanding officer of the unit, is to provide support to local disaster authorities when dealing with a potential WMD device. CST is designed to be the first military response team on the scene of a WMD−type disaster, with a response time of 90−minutes. From the time that its impressive fleet of vehicles drove up the hill to the designated area in the parking lot that served as a base, the CST was set up and ready to take care of personnel within 35 minutes.
Source: http://www.southernblackhillsweeklygroup.com/articles/2006/06/07/hot_springs/community/comm01.txt

[Return to top]

Information Technology and Telecommunications Sector

31. *June 08, CNET News* — **Microsoft drops PC sync from Vista.** Microsoft has dropped a feature from Windows Vista that would have allowed people running the new operating system to keep data synchronized among multiple PCs. The software maker said quality concerns were behind the decision to drop the feature, which allowed people to keep files up−to−date across multiple Vista machines. "While PC−to−PC sync is a great feature that improves productivity

and collaboration we don't have it at the quality level our customers demand," Microsoft said Wednesday, June 7 in a statement.
Source: http://news.com.com/Vista+gets+out+of+PC+sync/2100−1016_3−60 81232.html

32. *June 07, CNET News* — **Microsoft releases public download of Vista.** After months of limited testing, Microsoft made a beta version of Windows Vista publicly available for download on Wednesday, June 7. The company kicked off what it called its "Customer Preview Program," a testing period in which the software maker hopes millions of tech enthusiasts will kick the tires on the new operating system. People can either download the software from Microsoft's Website or pay a small fee to get it on DVD.
To download Microsoft Vista: http://www.microsoft.com/windowsvista/getready/default.mspx
Source: http://news.com.com/Microsoft+releases+public+download+of+Vi
sta/2100−1016_3−6081301.html?tag=nefd.top

33. *June 07, Reuters* — **Gartner: Chipmakers to see slower growth.** Sales growth of chips, also known as semiconductors, is expected to accelerate to 14 percent in 2008, then stalling in 2009 when annual growth will be less than one percent, Gartner said in a midyear update of its industry forecast. The outlook reflects a growing view that the industry, once subject to extreme boom−bust cycles, has shifted to slower, more stable growth as chips find their way into a vast array of consumer products from mobile phones to digital music players. Jim Tully, Gartner's head of semiconductor research, said the figures also showed that the $235 billion sector is heading for a new era of turbulence that will see 35 percent of existing chipmakers−−350 companies−−driven out of business or acquired by bigger rivals. "We've got markets slowing, costs increasing, chip prices falling and markets disappearing all over the place. That only leads to one conclusion: fewer types of chips being produced, but also fewer vendors," Tully said.
Source: http://news.com.com/Chipmakers+to+see+slower+growth−Gartner/
2100−1006_3−6081219.html

34. *June 07, Security Tracker* — **WinGate buffer overflow in HTTP proxy lets remote users execute arbitrary code.** A vulnerability was reported in WinGate. A remote user can send a specially crafted HTTP host name parameter value to trigger a buffer overflow in the HTTP proxy and execute arbitrary code on the target system. The code will run with the privileges of the target service.
Vulnerable software: WinGate version 6.1.1.1077
Solution: Please see source advisory.
Source: http://www.securitytracker.com/alerts/2006/Jun/1016239.html

35. *June 07, Secunia* — **Microsoft NetMeeting denial−of−service vulnerability.** Microsoft NetMeeting could be exploited by malicious users to cause a denial−of−service. The vulnerability is caused due to an error within the handling of certain received data. This can be exploited to overwrite application memory, which causes the application to crash or to consume a large amount of CPU resources.
Vulnerable software: Microsoft NetMeeting version 3.01.
Solution: Restrict use of the product to within trusted networks only.
Source: http://secunia.com/advisories/20477/

36.

June 07, IDG News Service — **Man charged with selling hacked VoIP services.** A Miami man was charged Wednesday, June 7 with stealing more than 10 million minutes of Voice over Internet Protocol (VoIP) telephone service and then selling them to unsuspecting customers for as little as US$0.004 per minute. Edwin Pena paid a Washington State computer hacker named Robert Moore about $20,000 to help him illegally route Internet telephone calls through the networks of more than 15 unnamed VOIP companies, according to a complaint filed with the U.S. Attorney's Office. Pena presented himself as a legitimate telecommunications wholesaler, while simultaneously using hacking techniques to steal networking services valued at as much as $300,000 from each of the carriers.
Source: http://www.infoworld.com/article/06/06/07/79053_HNvoiphack_1 .html

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of a buffer overflow vulnerability in Symantec Client Security and Symantec Antivirus Corporate Edition. Successful exploitation may allow a remote, unauthenticated attacker to execute arbitrary code with SYSTEM privileges. We are not aware of any public exploits at this time. For more information please review the following:

VU#404910 − Symantec products vulnerable to buffer overflow:
http://www.kb.cert.org/vuls/id/4049100

Symantec Advisory SYM06−010 − Symantec Client Security and Symantec AntiVirus Elevation of Privilege:
http://securityresponse.symantec.com/avcenter/security/Conte nt/2006.05.25.htmll

US−CERT will advise as more information becomes available.

Active Exploitation of a Vulnerability in Microsoft Word

US−CERT is aware of an increase in activity attempting to exploit a vulnerability in Microsoft Word. The exploit is disguised as an email attachment containing a Microsoft Word document. When the document is opened, malicious code is installed on the user's machine. More information about the reported vulnerability can be found in the following:

TRA06−139A − Microsoft Word Vulnerability:
http://www.us−cert.gov/cas/techalerts/TA06−139A.htmll

VU#446012 − Microsoft Word buffer overflow:
http://www.kb.cert.org/vuls/id/446012

Review the workarounds described in Microsoft Security Advisory 919637: http://www.microsoft.com/technet/security/advisory/919637.ms px

US−CERT strongly encourages users not to open unfamiliar or unexpected email attachments, even if sent by a known and trusted source. US−CERT will continue to update current activity as more information becomes available.

PHISHING SCAMS

US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT. http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 445 (microsoft−ds), 25 (smtp), 50497 (−−−), 4672 (eMule), 32788 (−−−), 24232 (−−−), 113 (auth), 80 (www) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

37. *June 08, Associated Press* — **Maryland bomb suspect planned to attack abortion clinic.** Federal authorities say man who made a bomb that damaged a Prince George's County house planned to use it to blow up an abortion clinic. Robert Weiler, 25, was arrested at a Garrett County, MD, rest stop on Interstate 68 around 12:30 a.m. EDT after he called agents from the Bureau of Alcohol, Tobacco, Firearms and Explosives to admit that he had made the bomb and had a gun that he planned to use in the attack, according to court documents. The device, a pipe bomb filled with nails which was stored in a closet at a Riverdale, MD, home, exploded several hours later as a bomb technician tried to defuse it. No one was injured, but the house was set on fire.
Source: http://www.wusatv9.com/news/news_article.aspx?storyid=50013

38. *June 07, USA TODAY* — **Security at malls, shopping centers inadequate, report says.** Major shopping centers have ranked near the top of potential terrorist targets, but there has been scant investment in additional security and emergency response plans are woefully inadequate, a

Police Foundation report has concluded. In the largest review of its kind since the September 11, 2001, attacks, the report, funded by the Department of Justice, found some shopping centers reporting 100 percent turnover in security officers each year. Robert Rowe of ASIS International, the nation's largest association of private security managers, said, “The complacency that exists" over the issue is disconcerting. "Since nothing has happened (since 9/11), security has become a less important priority.” Rowe's group assisted the Police Foundation, a law enforcement think tank, in obtaining federal funding for the report, which surveyed 33 state homeland security advisers and 120 security directors of some of the nation's largest indoor shopping centers. Malls have been the object of law enforcement concerns because of the vulnerability of their numerous entry and exit points. The shopping centers were not identified out of concern for making potential vulnerabilities public. The report's authors also visited eight U.S. malls and two shopping centers in Israel, where security precautions are among the most rigid in the world.
Source: http://www.usatoday.com/news/nation/2006−06−07−mall−security_x.htm

[Return to top]

General Sector

39. *June 08, Newsday (NY)* — **New York man tries to aid al Qaeda.** A Queens man is being held in London after he was indicted in Manhattan on charges that he provided military gear and other support to al Qaeda for use against U.S. forces in Afghanistan, officials disclosed on Wednesday, June 7. Syed Hashmi, 26, also known as Fahad, was arrested on Wednesday in London as he prepared to board a flight to Pakistan and was taken for a brief court appearance at Bow Street Magistrates Court where he refused to consent to extradition to the United States. Hashmi −− a native Pakistani who is a naturalized U.S. citizen and had been living in Queens −− was accused in the federal indictment of plotting with others to provide "material support or resources" to al Qaeda from January 2004 until last month The indictment stated that a key source of information for prosecutors was another person who had been arrested in a federal criminal case in Manhattan.
Source: http://www.newsday.com/news/nationworld/world/ny−nyterr08477 3340jun08,0,1566113.story?coll=ny−worldnews−print

40. *June 07, Reuters* — **Canada plot: Flight training link.** Canadian television reports that one member of a group of Toronto−area men now in custody on terror−related charges had enrolled in a flight training program as part of a plan to use aircraft in an attack on Canadian targets. Canadian Broadcasting Corporation (CBC), which cited allegations contained in court documents, said Wednesday, June 7, Amin Mohamed Durrani, 19, had enrolled in a training program at a Toronto−area college but then withdrew out of fear his activities would draw the attention of authorities. Durrani is one of 12 men and five youths being held after a weekend raid in and around Toronto. Several of the accused face charges of knowingly participating in a terrorist group, while six are charged with planning an explosion that could cause death or serious injury. The documents repeated allegations revealed by a lawyer at a court appearance Tuesday, June 6, that some in the group had planned to storm Parliament and take politicians hostage to force Canada to remove its troops from Afghanistan. Citing the documents, CBC said suspects were also alleged to have planned attacks against Toronto police stations using radio−controlled toys packed with explosives.

Source: http://www.cnn.com/2006/WORLD/americas/06/07/canada.terror.p lot.reut/index.html

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer